IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS

ERIK DAVIDSON, JOHN RESTIVO, and NATIONAL CENTER FOR PUBLIC POLICY RESEARCH,

Plaintiffs,

v.

GARY GENSLER and U.S. SECURITIES AND EXCHANGE COMMISSION,

Defendants.

Case No. 6:24-cv-197-ADA

AMICUS BRIEF OF THE AMERICAN SECURITIES ASSOCIATION, ATTORNEY GENERAL WILLIAM BARR, AND THE AMERICAN FREE ENTERPRISE CHAMBER OF COMMERCE

J. Michael Connolly
Steven C. Begakis
CONSOVOY MCCARTHY PLLC
1600 Wilson Blvd., Suite 700
Arlington, VA 22209
(703) 243-9423
mike@consovoymccarthy.com
steven@consovoymccarthy.com

Counsel for Amici Curiae

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES

REGULATIONS

OTHER AUTHORITIES

INTEREST OF AMICUS CURIAE[1]

The American Securities Association (ASA) is a trade association that represents the retail and institutional capital markets interests of regional financial services firms who provide Main Street businesses with access to capital and advise hardworking Americans how to create and preserve wealth. ASA's mission is to promote trust and confidence among investors, facilitate capital formation, and support efficient and competitively balanced capital markets. This mission advances financial independence, stimulates job creation, and increases prosperity. ASA has a geographically diverse membership base that spans the Heartland, Southwest, Southeast, Atlantic, and Pacific Northwest regions of the United States. ASA believes that the Commission's collection of personally identifiable information (PII) through the Consolidated Audit Trail (CAT) will create significant risks for investors by exposing them to warrantless government surveillance and cybercrime. These risks will undermine Main Street investor confidence and chill investment decisions, harming the capital markets that ASA seeks to promote. ASA has spoken out about the CAT for years and is also involved in other litigation challenging the SEC's actions concerning the CAT. *See ASA v. SEC*, No. 23-13396 (11th Cir.).

U.S. Attorney General William P. Barr served as the seventy-seventh and the eighty-fifth Attorney General of the United States. During these tenures, the Department of Justice steadfastly defended the rule of law, including the proper enforcement of federal statutes and the Fourth Amendment. General Barr has opposed the SEC's collection of PII through the

[1] This brief was not authored in whole or in part by counsel for any party and no person or entity other than *amici curiae* or their counsel has made a monetary contribution toward the brief's preparation or submission. All parties were notified of and consented to this brief.

CAT because it lacks congressional authorization; invites abusive investigations; creates a single repository that will be hacked, stolen, or misused; and clearly violates the Fourth Amendment's limits by collecting private information on tens of millions of investors without any connection to suspected wrongdoing. *See* Att'y Gen. William P. Barr, *The Securities and Exchange Commission Is Watching You*, The Wall Street Journal (Apr. 15, 2024), bit.ly/3Yvg2a7.

Formed in 2022, the American Free Enterprise Chamber of Commerce (AmFree) is a 501(c)(6) organization that represents hard-working entrepreneurs and businesses across all sectors to serve as the voice for pro-business and free market values. AmFree conducts research and develops policy initiatives designed to support free, fair, and open markets that spur economic growth. AmFree's members have been saddled with overly burdensome regulations and harmed by the expansion of the federal regulatory state. They are concerned about this relentless regulatory advance and its effect on the U.S. financial services sector, which undermines the ability of firms to provide market access to ordinary Americans and threatens the status of America's financial markets. AmFree files amicus briefs in important regulatory and constitutional cases to support reining in the administrative state and to promote constitutional accountability.

INTRODUCTION

Defendants try to paint the Consolidated Audit Trail (CAT) as a mundane enforcement program that raises few legal and privacy concerns. Not so. *Amici* write to highlight several reasons why the CAT's collection of personally identifiable information (PII) raises a major question and violates the Fourth Amendment.

The major questions doctrine was designed for cases like this. The "size [and] scope" of the CAT's collection of investors' PII represents an "unprecedented" threat to investor safety, privacy, and freedom. *Ala. Ass'n of Realtors v. HHS*, 594 U.S. 758, 765 (2021). "[I]n its [90 years] of existence, [the SEC] has never before adopted a broad [surveillance] regulation of this kind." *NFIB v. OSHA*, 595 U.S. 109, 119 (2022). There are over 100 million American investors, and all of them "fal[l] within" the CAT dragnet. *Ala. Realtors*, 594 U.S. at 764. The "'economic impact'" of this undertaking—especially from security breaches—is "significant." *Biden v. Nebraska*, 143 S. Ct. 2355, 2373 (2023). And "the issues at stake" in the mass-collection of PII "are not merely financial." *Ala. Realtors*, 594 U.S. at 764. The CAT's ability to monitor every trade and to link each trade to individual investors in real time gives the SEC "unheralded power to regulate 'a significant portion of the American economy,'" and will "bring about an enormous and transformative expansion in [the SEC's] regulatory authority." *Util. Air Regul. Grp. v. EPA*, 573 U.S. 302, 324 (2014). It will "'significantly alter … the power of the Government over private property" and individual privacy. *Ala. Realtors*, 594 U.S. at 764.

The CAT's collection of investors' PII has also been "the subject of an 'earnest and profound debate' across the country." *Gonzales v. Oregon*, 546 U.S. 243, 267 (2006). For years this issue has provoked opposition from members of Congress and the public because of dire concerns about cybersecurity and privacy. This is further evidence of a major question because it shows that "the basic and consequential tradeoffs inherent in [the CAT] … are ones that Congress would likely have intended for itself," *Biden*, 143 S. Ct. at 2375 (cleaned up), making "'the claimed delegation all the more suspect,'" *West Virginia v. EPA*, 597 U.S. 697, 732 (2022).

The CAT's collection of PII also violates the Fourth Amendment. Requiring every American investor to turn over their personal data with no suspicion of wrongdoing not only undermines settled expectations of privacy that undergird the investor-broker relationship but also fails to satisfy the constitution's bare minimum requirement of "reasonableness." The Court should deny the motions to dismiss and grant the Plaintiffs' motion for a stay and preliminary injunction.

ARGUMENT

I. The legality of SEC's collection of PII through the CAT is a major question.

A. The CAT's unprecedented collection of investors' PII has vast political and economic significance.

The CAT is a "comprehensive surveillance database," not "an innocuous repository of dry economic data." Comm'r Hester M. Peirce, *Statement of Hester M. Peirce in Response to Release No. 34-88890; File No. S7-13-19* (May 15, 2020), bit.ly/3gUHeqp (Peirce Statement). This database will contain a "comprehensive record of decisions made by millions of Americans," including "every equity and option trade and quote, from every account at every broker, by every investor." *Id.* Access to this vast trove of data is minimally restricted, with "[t]housands of Commission staff and employees of the participants" having potential access. *Id.* The CAT "is required to be able to support a minimum of 3,000 users at one time," *id.*, who have "access 'to every trade, from every account, from every broker, for every retail investor in America.'" SIFMA, *Senate Banking Committee Hearing on the CAT* (Oct. 22, 2019), bit.ly/33hrSqM (quoting Sen. Tom Cotton). The Commission and self-regulatory organizations (SROs), such as the national stock exchanges and FINRA, can access this data for "surveillance [or] regulatory purposes." 17 C.F.R. §242.613(e)(4)(i)(A); *see* CAT NMS Plan §6.5(c), bit.ly/4caHuNy.

Contrary to the SEC's effort to now downplay the size and scope of the CAT, *see* SEC Mot. 26-32 (likening the CAT to "prior audit trails"), the SEC has long acknowledged that this massive surveillance system is "'unprecedented.'" Chair Gary Gensler, *Statement on CAT Funding* (Sept. 6, 2023), bit.ly/46pLLeR (quoting Chariman Mary L. Shapiro, *Opening Statement at SEC Open Meeting: Consolidated Audit Trail* (July 11, 2012), bit.ly/3yBoI40). It has vast political and economic significance for several reasons.

1. The CAT's collection of PII threatens individual freedom.

First, the CAT's collection of PII has vast political significance because of the profound risks that it poses to individual freedom. "The non-financial costs of being surveilled reach to the very core of our humanity." Peirce Statement. Freedom of thought, expression, and action are "the basis of our national strength and of the independence and vigor of Americans." *Tinker v. Des Moines Indep. Cmty. Sch. Dist.*, 393 U.S. 503, 508-09 (1969). But "[u]ntargeted government surveillance programs, even well-intentioned ones, threaten that freedom." Peirce Statement. That is because "[a]wareness that the government may be watching chills" individuals' activities. *United States v. Jones*, 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring).

There is a reason why sensitive economic data that an investor "intend[s] to be kept confidential" is her "property" and must be respected as such. *Carpenter v. United States*, 484 U.S. 19, 28 (1987). Economic transactions, including investment decisions, can "express a view of how markets work, a determination on the efficiency of markets, expectations about the future, or even a moral philosophy," and thus "offer a window into a person's deepest thoughts and core values." Peirce Statement. For example, "an investor may purchase shares of a clothing company because he likes the political messages of its celebrity spokesperson or

shares of a restaurant chain because it donates to his favorite charity." *Id.* Another investor "may choose to avoid or sell companies that are associated with things he opposes," such as carbon emissions, tobacco, and guns. *Id.* Individuals have a right to expect their views on sensitive and emotional issues without being tracked and recorded by the government. *See Carpenter v. United States*, 585 U.S. 296, 311 (2018) (the fact that "records are generated for commercial purposes … does not negate [an] anticipation of privacy").

Investors may also "fear rebukes from other people [for their] trading decisions." Peirce Statement. They could face public pressure for investing in energy companies, cigarette manufacturers, or weapons makers, or be publicly shamed for not investing in companies that score high on Environmental, Social, and Governance (ESG) factors. *See* Comm'r Hester M. Peirce, *Scarlet Letters: Remarks Before the American Enterprise Institute*, (June 18, 2019), bit.ly/3pCbaMh. "[I]n our modern corporate ESG world, there is a group of people who take the lead in instigating their fellow citizens into a frenzy of moral rectitude. Once worked up, however, the crowd takes matters into its own brutish hands and finds many ways to exact penalties from the identified wrongdoers." *Id.*

Because human dignity requires that individuals have "personal privacy" over who they support with their economic transactions, *Sorrell v. IMS Health Inc.*, 564 U.S. 552, 579-80 (2011), investors are entitled to invest based on their moral, ethical, or religious beliefs without making a public statement or coming under perpetual surveillance. But the CAT's "compelled disclosure" of investors' transactions will lead investors to "fear … exposure of their beliefs … [and] the consequences of this exposure." *NAACP v. Ala. ex rel. Patterson*, 357 U.S. 449, 462-63 (1958). And that fear is not unreasonable. "One can imagine a future in which a delectably

large database of trades becomes a tool for the government to single people out for making trading decisions that reflect—or are interpreted to reflect—opinions deemed unacceptable in the reigning gestalt." Peirce Statement. "[O]ur Constitution was designed to avoid these ends by avoiding [their] beginnings." *W. Va. State Bd. of Educ. v. Barnette*, 319 U.S. 624, 641 (1943).

The CAT's unprecedented infringement on freedom and privacy also has constitutional dimensions, which further highlights its vast political significance. "[T]he individual interest in avoiding disclosure of personal matters" is at the heart of the constitutional right to privacy. *Whalen v. Roe*, 429 U.S. 589, 599 (1977). This includes a "constitutionally protected interest in the confidentiality of personal financial information." *Statharos v. N.Y.C. Taxi & Limo. Comm'n*, 198 F.3d 317, 322-23 (2d Cir. 1999); *see also Cal. Bankers Ass'n v. Shultz*, 416 U.S. 21, 78-79 (1974) (Powell, J., concurring) ("Financial transactions can reveal much about a person's activities, associations, and beliefs. At some point, governmental intrusion upon these areas would implicate legitimate expectations of privacy.").

Similarly, "[t]he First Amendment prohibits the use of compulsion to exact from individuals (or groups) the wholesale disclosure of their associational ties where such inquiry is [n]ot germane to the determination of whether a crime has been committed." *Reporters Comm. for Freedom of Press v. AT&T Co.*, 593 F.2d 1030, 1054 n.82 (D.C. Cir. 1978). And, of course, the CAT data will "offer a window into [investors'] deepest thoughts and core values" and often reflect their "moral, ethical, or religious beliefs." Peirce Statement.

Government actions that infringe on the right to privacy or the First Amendment are subject to heightened scrutiny. *See Statharos*, 198 F.3d at 324; *John Doe No. 1 v. Reed*, 561 U.S. 186, 196 (2010). But the sweeping and invasive data harvesting that the Commissions plans to

undertake cannot survive such scrutiny. Requiring everyday Americans to disclose sensitive information without any reasonable suspicion of wrongdoing is far from narrowly tailored and furthers no government interest.

2. The CAT's collection of PII risks improper enforcement.

Adding to its vast political significance, the CAT's collection of PII will also create an enormous data pool that will enable "[s]taff at the Commission and at the exchanges [to] wade through the data pool to troll for securities violations." Comm'r Hester M. Peirce, *Intellectual Siren Song* (Sept. 18, 2020), bit.ly/3lT0wyN. This tracking of "unsuspected and unsuspecting Americans' every move in the hopes of catching them in some wrongdoing" is not "consistent with the principles undergirding the Constitution." *Id.* It is blackletter law that "[a]gencies are … not afforded 'unfettered authority to cast about for potential wrongdoing.'" *CFPB v. Accrediting Council for Indep. Colls. & Schs.*, 854 F.3d 683, 689 (D.C. Cir. 2017).

The significance of this threat has increased with the advent of artificial intelligence. The Commission has already signaled its plans to use AI in the CAT database to go fishing for potential enforcement leads. *See* Comm'r Caroline A. Crenshaw, *Statement Regarding the Order Approving an Amendment to the National Market System Plan Governing the Consolidated Audit Trail* (Sept. 6, 2023), bit.ly/4cef98W. It is easy to imagine how this sci-fi experiment could go wrong. AI algorithms have well-known shortcomings: they make mistakes, do not always account for every relevant factor, and do not always operate with transparency. *See, e.g.*, Mike Thomas, *14 Risks and Dangers of Artificial Intelligence (AI)*, BuiltIn (Jul. 25, 2024), bit.ly/4dcsMqE. These limitations make it likely that federal agents will open investigations into countless innocent investors based on inadequate AI queries, incomplete AI analyses, or incorrect AI conclusions.

Even the threat of enforcement will cause great harm to everyday Americans. The SEC can coerce individuals into justifying their action, "potentially at great expenses," even if those individuals are innocent. Comm'r Hester M. Peirce, *This CAT is a Dangerous Dog*, RealClearPolicy (Oct. 9, 2019), bit.ly/3fTxTxE; *see, e.g.*, Judith Bellamy Peck, *The Ninth Circuit's Requirement of Notice to Targets of Third Party Subpoenas in SEC Investigations—A Remedy Without a Right*, 59 Wash. L. Rev. 617, 619 (1984) ("Merely being made the subject of an SEC investigation may involve high costs."). The financial, reputational, and operational harms to businesses and individuals from SEC investigations can be ruinous. The SEC does not have to formalize punishment in these circumstances. The process itself becomes the punishment.

3. The CAT's collection of PII increases the risk of cybercrime.

Then there is the CAT's vast economic significance. Putting aside the CAT's *billions* of dollars in operating and compliance costs, *see, e.g.*, PI Mot. 11-12; Opening Br., *ASA v. SEC*, No. 23-13396, Dkt. 49 at 21-22 (11th Cir. Feb. 8, 2024), the CAT's collection of PII will leave everyday Americans at the mercy of cybercriminals. "[T]he risks to the American investor" from "[e]very trade from every account at every broker for every retail investor in the U.S. recorded in a single place … are staggering." Comm'r Hester M. Peirce, *This CAT is a Dangerous Dog*, RealClearPolicy (Oct. 9, 2019), bit.ly/3fTxTxE.

To begin, security breaches could "leak highly confidential information about trading strategies or positions, which could be deleterious for market participants' trading profits and client relationships." *Joint Industry Plan; Order Approving the National Market System Plan Governing the Consolidated Audit Trail*, 81 Fed. Reg. 84696, 84875 (Nov. 23, 2016); *see, e.g.*, *Front Running*, Corporate Financial Institute, bit.ly/3ku91i1 (explaining how investors will purchase securities

"based on advanced non-public information"). Moreover, exposing the private trading patterns of institutional investors could reveal proprietary trading strategies, thus undermining investments into sophisticated trading methods. *See* Jane Croft, *Citadel Securities Sues Rival Over Alleged Trading Strategy Leak*, Financial Times (Jan. 10, 2020), on.ft.com/3nkbFZs (discussing the alleged theft of Citadel Securities' trading algorithms, which cost $100 million to develop).

The information harvested by the CAT goes beyond just trading strategies, and a data breach could "expose proprietary information about the existence of a significant business relationship with either a counterparty or client, which could reduce business profits." *Joint Industry Plan*, 81 Fed. Reg. at 84874. For example, a government report was recently leaked and disclosed that "a number of banks … continued to profit from illicit dealings with disreputable people and criminal networks despite previous warnings from regulators." *Bank Shares Slide on Report of Rampant Money Laundering*, The Associated Press (Sep. 21, 2020), bit.ly/3ppBNEk. Unsurprisingly, these leaks caused the companies' stock value to drop. *Id.* Each leak from the CAT could cause similar or greater harms to investors.

There are also costs to leaking confidential enforcement information. A breach could "compromise regulatory efforts or lead to speculation that could falsely harm the reputation of market participants and investors." *Joint Industry Plan*, 81 Fed. Reg. at 84875. For example, a group of government officials recently leaked the existence of an FTC investigation into Facebook (now known as Meta) and caused the company's stock to "briefly f[a]ll into bear market territory, more than 20 percent off its 52-week high." Sara Salinas, *Facebook Stock Slides After FTC Launches Probe of Data Scandal*, CNBC (Mar. 26, 2018), cnb.cx/38AOB4y.

A data breach could also allow cybercriminals to break into the brokerage accounts of everyday Americans and steal their investments. *See, e.g.*, Casey Bond, *How Hackers Can Use Your Boarding Pass to Easily Steal Personal Information*, HuffPost (Dec. 5, 2019), bit.ly/38HkYyy; *Why Your Birth Date is Important to Hackers?*, Hackology (June 24, 2018), bit.ly/3lx2eFR. For example, when in 2020 a group of hackers infiltrated the mobile investment platform of Robinhood Markets, "2,000 Robinhood Markets accounts were compromised" and cybercriminals were able to "siphon off customer funds." Sophie Alexander, *Robinhood Internal Probe Finds Hackers Hit Almost 2,000 Accounts*, Bloomberg Wealth (Oct. 15, 2020), bloom.bg/35Gy7oG. "Several victims said they found no sign of criminals compromising their email accounts." *Id.* "And some said their brokerage accounts were accessed even though they had set up two-factor authentication." *Id.*

And the costs of CAT security breaches will only increase over time. Cybercrime is constantly increasing in frequency, sophistication, and severity. *See, e.g.*, *CrowdStrike Global Threat Report Reveals Big Game Hunting, Telecommunication Targeting Take Center Stage for Cyber Adversaries*, CrowdStrike (Mar. 23, 2020), bit.ly/32QLxhz. And nobody is safe. "[E]ven the most security-minded federal agencies are struggling to defend" against cybercriminals. Timothy Gardner & Raphael Satter, *U.S. Energy Dept Gets Two Ransom Notices as MOVEit Hack Claims More Victims*, Reuters (Jun. 16, 2023), bit.ly/3yFnHIe. For example, hackers recently breached the "National Nuclear Security Administration, which maintains the U.S. nuclear weapons stockpile." Natasha Bertrand & Eric Wolff, *Nuclear Weapons Agency Breached Amid Massive Cyber Onslaught*, Politico (Dec. 17, 2020), bit.ly/4cxdAmB. Former SEC Chairman Jay Clayton has sensibly recognized that "[c]yber risks … [are] there, and they're there more than

ever." Kevin Stankiewicz & Bob Pisani, *Cybersecurity Threats to Corporate America Are Present Now 'More Than Ever,' SEC Chair Says*, CNBC (Nov. 2, 2020), cnb.cx/36w6sqL.

Recent history is replete with examples of devastating cybercrime. Just days before this case was filed, "[m]illions of current and former AT&T customers learned … that hackers … stol[e] their personal information and [were] sharing it on the dark web." Khristopher J. Brooks, *What Customers Should Know About AT&T's Massive Data Breach*, CBS News (Apr. 11, 2024), bit.ly/3AfYCUT. The data breach "affected about 7.6 million current and 65.4 million former AT&T customers." *Id.* Likewise, in 2019 and 2020, Chinese hackers victimized "over 100 … companies in the United States and abroad, including software development companies, computer hardware manufacturers, telecommunications providers, social media companies, video game companies, non-profit organizations, universities, think tanks, and foreign governments, as well as pro-democracy politicians and activists in Hong Kong." Press Release, *Seven International Cyber Defendants, Including "Apt41" Actors, Charged in Connection With Computer Intrusion Campaigns Against More Than 100 Victims Globally*, U.S. Dep't of Justice (Sept. 16, 2020), bit.ly/2HmrhMw. They stole reams of private information, including "customer account dat[a] and valuable business information." *Id.*

Then there was the Equifax hack, an "'organized and remarkably brazen criminal heist of sensitive information of nearly half of all Americans … by a unit of the Chinese military.'" U.S. Dep't of Justice, *Chinese Military Personnel Charged With Computer Fraud, Economic Espionage and Wire Fraud for Hacking Into Credit Reporting Agency Equifax* (Feb. 10, 2020), bit.ly/3mInj0I. After piercing Equifax's security, members of the Chinese People's Liberation Army "were able to download and exfiltrate" enormous amounts of data, including personal and financial

information. *Id.* This was not an isolated incident. In 2018, the Chinese government hacked Marriott International, Inc., and stole reams of personal information belonging to up to 500 million people. *See* Eric Geller, *Pompeo Says China Hacked Marriott*, Politico (Dec. 12, 2018), politi.co/3mF6eow. And in 2015 the Chinese government hacked the Office of Personnel Management. They stole "Social Security numbers and other sensitive information on 21.5 million people who [had] undergone background checks for security clearances" as well as other "data on about 4.2 million current and former federal workers," in total impacting "almost 7 percent of the U.S. population." Patricia Zengerle & Megan Cassella, *Millions More Americans Hit by Government Personnel Data Hack*, Reuters (July 9, 2015), reut.rs/3oLxV0b.

The SEC knows about these threats from its own experience. After a recent inspector-general review found that the SEC is not compliant with federal cybersecurity standards, hackers commandeered the SEC's X (formerly Twitter) account to spike the price of Bitcoin. *See* Austin Weinstein & Jamie Tarabay, *SEC Had a Fraught Cyber Record Before X Account Was Hacked*, Bloomberg Law (Jan. 12, 2024), bit.ly/3WUmBlp. And in 2019, two Ukrainian men were indicted for "a large-scale, international conspiracy to hack into the [SEC's] computer systems and profit by trading on critical information they stole." Press Release, *Two Ukrainian Nationals Indicted in Computer Hacking and Securities Fraud Scheme Targeting U.S. Securities and Exchange Commission*, U.S. Dep't of Justice (Jan. 15, 2019), bit.ly/2J4SEvh. These men "hacked into the SEC's [EDGAR] system and stole thousands of files … [and] then profited by selling access to the confidential information in these reports and trading on this stolen information prior to its distribution to the investing public." *Id.*

Finally, the very individuals who operate the CAT could acquire and trade investor data for their own gain and even vindictively harm an investor's reputation by leaking sensitive information about that investor's controversial trades. Sadly, government officials have a history of leaking sensitive, private information to the public. *See, e.g.*, Kim Zetter, *Bradley Manning to Face All Charges in Court-Martial*, Wired (Feb. 3, 2012), bit.ly/34Ft8VK. And one study found that 42% of government officials believe that it is appropriate to leak information to the press. *See* David E. Pozen, *The Leaky Leviathan: Why the Government Condemns and Condones Unlawful Disclosures of Information*, 127 Harv. L. Rev. 512, 528 (2013).

B. The SEC's collection of PII through the CAT has been the subject of an earnest and profound debate across the country.

The vast political and economic significance of the CAT is further corroborated by the intense controversy that has consistently surrounded the project from the start. After the SEC first approved the CAT in November 2016, *see Joint Industry Plan*, 81 Fed. Reg. 84696, the CAT immediately "started to attract an enormous amount of criticism and concern regarding cybersecurity." James Rundle & Anthony Malakian, *CAT's Tale: How Thesys, the SROs and the SEC Mishandled the Consolidated Audit Trail*, WatersTechnology (Feb. 14, 2019), bit.ly/4ceSiu3. This concern was heightened by the high-profile data breaches discussed above. *See id.*

Congress then took notice, holding multiple hearings into "what information the CAT would be collecting, and how it would be protected." *Id.* In these hearings, witnesses repeatedly raised concerns about the CAT's collection of traders' personal and financial information. *See, e.g.*, *Implementation and Cybersecurity Protocols of the Consolidated Audit Trail*, Hearing before the U.S. H.R. Comm. on Fin. Servs. (Nov. 30, 2017), bit.ly/2ZqAl8p, *id.* (testimony of Lisa Dolly, CEO of SIFMA), bit.ly/2ASDlCp (warning Congress that "the CAT will contain a significant

amount of sensitive information," including the "[PII] of individual customers," and "the SEC and the SROs" have not "ma[de] the case" that this "is required for effective surveillance"); *id.* (testimony of Chris Concannon, President and COO of Cboe Global Markets, Inc.), bit.ly/31PwUuS (raising "concern[s] about the risks associated with storing PII in the CAT database"); *see also id.* (statement of Rep. Bill Huizenga), bit.ly/3dKWFi5 (identifying "very serious concerns about the security of such extraordinary amounts of [PII] being collected").

In 2019, the Commission received letters and comments urging the agency to stop collecting PII through the CAT. In July 2019, a coalition of senators sent a letter to the Commission expressing grave national security concerns:

> We write to you regarding the national security risk China poses to all American investors because of the planned collection of their personally identifiable information (PII) by the Consolidated Audit Trail (CAT) database. … Given the aggressive nature of the Chinese Communist Party's cyber agenda and the risk this presents to the American people, we are asking the Commission to prohibit the collection of *any* retail investor PII by the CAT. … [W]e are worried that including the PII of every American with money in the stock market will create an easy target for China's cyber-attack initiatives.

Sen. John Kennedy, et al., Letter to SEC (July 24, 2019), bit.ly/2A1E5oi. Representatives in the House would also propose several pieces of legislation to prohibit the CAT from collecting PII. *See, e.g.*, H.R. 4551 (2023); H.R. 2039 (2021); H.R. 4785 (2018).

ASA also urged the Commission on multiple occasions to stop collecting PII. *See* ASA, Comment on SEC Proposed Rulemaking (Nov. 30, 2020), bit.ly/2LFM5AM; ASA, Comment on SEC Proposed Rulemaking (Oct. 28, 2019), bit.ly/2Rg5k2V; ASA, Letter to SEC and CAT NMS Plan Participants (May 16, 2019), bit.ly/3egvJqR; ASA, Letter to SEC (Feb. 25, 2019), bit.ly/3iQ7e7A. ASA explained that (1) PII collection "will do nothing to support the mission of the CAT and will only subject the PII of millions of Americans to theft from

cybercriminals"; (2) there is "no compelling reason" to collect PII; (3) "the costs associated with collecting PII vastly outweigh any benefit to investors or the SEC's ability to oversee markets"; and (4) "[t]he SEC does not need PII to conduct market surveillance and police bad actors." ASA, Comment on SEC Proposed Rulemaking (Oct. 28, 2019), bit.ly/2Rg5k2V.

Others made similar arguments and requests. The ACLU wrote a letter to Chairman Clayton expressing dismay that "the CAT will collect and store far too much [PII]" and urging the Commission to "consider further measures to limit the personal information maintained by the CAT." ACLU, Letter to SEC (Dec. 16, 2019), bit.ly/2Nk9oh8. And Commissioner Peirce criticized the CAT's enormous collection of customers' personal and financial information, arguing that it would create a database "so vast and so attractive to hackers that it will be hard to protect" from cybercriminals. Comm'r Hester M. Peirce, *This CAT is a Dangerous Dog*, RealClearPolicy (Oct. 9, 2019), bit.ly/3fTxTxE. Commissioner Peirce has repeatedly raised these concerns. *See, e.g.*, Peirce Statement; Comm'r Hester M. Peirce, *Statement on the Order Granting Temporary Conditional Exemptive Relief from Certain Requirements of the National Market System Plan Governing the Consolidated Audit Trail* (July 8, 2022), bit.ly/3ydnR9N.

Even the SEC was forced to weigh in and acknowledge the widespread and serious public concerns about cybersecurity. Former Chairman Jay Clayton repeatedly said that he agreed that there are valid "concerns … about the protection of any investors' PII that would be stored in the CAT." *Testimony on "Oversight of the Securities and Exchange Commission," Before the U.S. Senate Committee on Banking, Housing, and Urban Affairs* at 18, Chairman Jay Clayton, U.S. Sec. & Exch. Comm'n (Dec. 10, 2019), bit.ly/2TmHMMz; *see, e.g.*, Chairman Jay Clayton,

Statement on Status of the Consolidated Audit Trail (Sept. 9, 2019), bit.ly/2YZUfa; Chairman Jay Clayton, *Statement on Status of the Consolidated Audit Trail* (Nov. 14, 2017), bit.ly/3SUfRSf.

* * *

Because the CAT's collection of PII raises a major question, and the SEC has already admitted that Congress did not give it "express authorization for [the] CAT," *Joint Industry Plan; Order Approving an Amendment to the National Market System Plan Governing the Consolidated Audit Trail; Notice*, 88 Fed. Reg. 62628, 62673 (Sept. 12, 2023), as is required by the major questions doctrine, *see, e.g.*, *West Virginia*, 597 U.S. at 723, the Court should deny the motions to dismiss and grant the Plaintiffs' motion for a stay and preliminary injunction.

II. The SEC's collection of PII violates the Fourth Amendment.

On top of showing a lack of statutory authority, Plaintiffs have stated a claim that the CAT's collection of PII violates the Fourth Amendment. A search or seizure within the Fourth Amendment occurs "when an expectation of privacy that society is prepared to consider reasonable is infringed." *United States v. Jacobsen*, 466 U.S. 109, 113 (1984). This happens when an individual "'seeks to preserve something as private'" and society "'recognize[s]'" that expectation as reasonable. *Carpenter*, 585 U.S. at 304. Courts across the country have repeatedly recognized that compelled production of data implicates the Fourth Amendment. *See, e.g.*, *City of L.A., Calif. v. Patel*, 576 U.S. 409, 412 (2015) (a law that required hotels to make their guest registries available to the police on demand for inspection violated the Fourth Amendment); *Airbnb, Inc. v. City of N.Y.*, 373 F. Supp. 3d 467, 483 (S.D.N.Y. 2019) (a law that required AirBnB to produce its user records was an "event that implicate[d] the Fourth Amendment").

The PII that the SEC will collect through the CAT is information that companies and individuals aim to keep private. Financial firms prioritize customer privacy through various measures such as privacy statements, safeguards, and advanced technology. This commitment is crucial for maintaining client relationships, as customers are justifiably concerned about sharing personal and financial information.

The expectation of privacy in investor PII is one that society recognizes as reasonable. Investors have many valid reasons for wanting to keep this data private, including avoiding social stigma, protecting business interests, and preventing cybercrime. This expectation is reinforced by Commission regulations like 17 C.F.R. §248.30(a), which requires broker-dealers to adopt safeguards for customer records. Other laws also reflect society's recognition of the need to protect similar types of sensitive information. *See, e.g.*, 15 U.S.C. §6803(c) (requiring financial institutions to disclose to their customers how they will "protect the confidentiality and security of nonpublic personal information"); 42 U.S.C. §1320d-6 (prohibiting "[w]rongful disclosure of individually identifiable health information").

The CAT's collection of investors' PII is not "reasonable" because it is not "sufficiently limited in scope, relevant in purpose, and specific in directive." *See v. City of Seattle*, 387 U.S. 541, 544 (1967). The CAT will collect the personal data of every single American investor who buys or sells a security, allowing the SEC to reconstruct and store every investor's entire financial portfolio. And the SEC is doing this preemptively, regardless of whether it has any particularized or even general suspicion that an investor has violated any securities laws, and regardless of whether the SEC has any desire to use an investor's data for market analysis or reconstruction or other regulatory efforts. This is not even close to properly tailored.

For example, in *Airbnb v. City of New York*, a federal court found that a New York City ordinance requiring hotel booking companies to report the personal information of their hosts and the hosts' guests—for every booking made through their platforms—violated the Fourth Amendment. 373 F. Supp. 3d at 481-95. The Court had "little difficulty" finding that the ordinance was a search or seizure within the Fourth Amendment because Airbnb had a "privacy interest in the data" of its users. *Id.* at 482-86. The ordinance was not reasonable because "the scale of the production that the Ordinance compels … [was] breathtaking," making it "the antithesis of a targeted administrative subpoena for business records" and "devoid of any tailoring." *Id.* at 490-91. That the ordinance would "facilitate [the City's] enforcement efforts" was of no moment. *Id.* at 491-95 "[T]he test of reasonableness is not whether an investigative practice maximizes law enforcement efficacy." *Id.* at 492.

Carpenter also is instructive. There, the federal government obtained a conviction by using cell-cite data to track and produce maps of the defendant's movements, which allowed the government to prove that the defendant's phone was "near four of the charged robberies." *Carpenter*, 585 U.S. at 302-03. The Court held that "the ability to chronicle a person's past movements through the record of his cell phone signals" implicates the Fourth Amendment, such that "when the Government accessed [cell-site data] from the wireless carriers, it invaded [the defendant's] reasonable expectation of privacy in the whole of his physical movements." *Id.* at 309, 313. It also rejected the argument that cell-site data were business records that deserved no Fourth Amendment protection. *See id.* at 313-16.

The CAT's collection of investors' PII also violates the Fourth Amendment because it fails to allow "precompliance review before a neutral decisionmaker." *Patel*, 576 U.S. at 420.

"[A]bsent consent, exigent circumstances, or the like, in order for an administrative search to be constitutional, the subject of the search must be afforded an opportunity to obtain precompliance review." *Id.* For example, in *Patel*, the City of Los Angeles required "hotel operators to record information about their guests," such as their name, address, license plate number, room information, and method of payment, and to make this information "available to any officer of the Los Angeles Police Department for inspection." *Id.* at 412-13. If a hotel owner "refuse[d] to give an officer access to his or her registry," that owner could be "arrested on the spot," meaning that the owner would have no opportunity for judicial review. *Id.* at 421. The Supreme Court held that this requirement was unconstitutional, since "business owners cannot reasonably be put to this kind of choice." *Id.* Likewise here, neither brokers nor individual investors can opt out of the CAT unless they stop trading.

"The CAT program clearly violates [the Fourth Amendment's] limits by collecting private information on tens of millions of investors without any connection to suspected wrongdoing." Att'y Gen. Barr, *The Securities and Exchange Commission Is Watching You*. "The crux of the SEC's argument" for the CAT "is that it could investigate things more easily if it weren't limited to gathering investor information on a case-by-case basis after suspected wrongdoing took place." *Id.*; *see, e.g.*, SEC Mot. 30. "But the whole point of the Fourth Amendment is to make the government less efficient by making it jump through hoops when it seeks to delve into private affairs." Att'y Gen. Barr, *The Securities and Exchange Commission Is Watching You*.

CONCLUSION

The Court should deny Defendants' motions to dismiss and grant the Plaintiffs' motion for a stay and preliminary injunction.

Dated: August 22, 2024

Respectfully submitted,

/s/ J. Michael Connolly

J. Michael Connolly (VA Bar No. 77632)
Steven C. Begakis (TX Bar No. 24139306)
CONSOVOY MCCARTHY PLLC
1600 Wilson Blvd., Suite 700
Arlington, VA 22209
(703) 243-9423
mike@consovoymccarthy.com
steven@consovoymccarthy.com

Counsel for Amici Curiae

CERTIFICATE OF SERVICE

I hereby certify that a true and correct copy of the foregoing has been served on counsel of record via the Court's electronic filing and service on August 22, 2024.

/s/ J. Michael Connolly